IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
W. Dale Hopkins, et al. § Confirmation No. 9964
§
Serial No.: 10/749,200 § Group Art Unit: 2439
§
Filed: December 31, 2003 § Examiner: Wang, Harris C.
§
For: PIN VERIFICATION USING CIPHER § Atty Docket:
BLOCK CHAINING § 200309348-1
§ HPQB:0194

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF TRANSMISSION OR MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted by facsimile to the United States Patent and Trademark Office in accordance with 37 C.F.R. § 1.6(d), or is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.6(a)(4), or is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

May 25, 2010	/Nathan E. Stacy/
Date	Nathan E. Stacy, Reg. No. 52,249

APPEAL BRIEF PURSUANT
TO 37 C.F.R. §§ 41.31 AND 41.37

This Appeal Brief is being filed in response to the Final Office Action mailed on December 28, 2009, and in furtherance of a Notice of Appeal filed March 25, 2010.

1. **REAL PARTY IN INTEREST**

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Dr. W, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

2. **RELATED APPEALS AND INTERFERENCES**

The Appellants are unaware of any other appeals or interferences related to this Appeal. The undersigned is Appellants' legal representative in this Appeal.

3. **STATUS OF CLAIMS**

Claims 1-31 are currently pending, are currently under rejection and, thus, are the subject of this appeal.

4. **STATUS OF AMENDMENTS**

There are no outstanding amendments to be considered by the Board.

5. **SUMMARY OF CLAIMED SUBJECT MATTER**

The Application contains seven independent claims, namely, claims 1, 11, 20, and 28-31, all of which are the subject of this Appeal. As an example, the independent claims relate generally to data security techniques and Personal Identification Number (PIN) verification. *See* Application, p.1, ll. 12-24; p. 2, ll. 25-27. The application also contains dependent claims 2-10, 12-19, and 21-27. The subject matter of independent claims 1, 11, 20, and 28-31 is summarized below. The subject matter of dependent claims 2, 4, 5, 6, 14, 15, 22, and 23 is also summarized below.

With regard to independent claim 1, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 1 recites a Personal Identification Number (PIN) verification apparatus (*e.g.*, 100) including a plurality of cipher blocks (*e.g.*, 102A, B) linked in a Cipher Block Chain (CBC) and keyed with a secret PIN Verification Key (PVK). *See* Application, p. 4, ll. 3-7; Figure 1A. The apparatus includes a first input block (*e.g.*, 104A) coupled to a first cipher block (*e.g.*, 102A) in the CBC chain that receives a first plaintext block derived from a secret Personal Identification Number (PIN). *See id.* at p. 4, ll. 7-9; Figure 1A. The apparatus also includes a second input block (*e.g.*, 104B) coupled to a second cipher block (*e.g.*, 102B) in the CBC chain that receives a second plaintext block derived from a non-secret entity-identifier independent of the PIN and receives ciphertext from a cipher block (*e.g.*, 102A, B) in the CBC chain. *See id.* at p. 4, ll. 9-11; Figure 1A.

With regard to independent claim 11, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 11 recites a method (*e.g.*, 200) for Personal Identification Number (PIN) verification including linking (*e.g.*, 202) a plurality of cipher blocks in a Cipher Block Chain (CBC). *See* Application, p. 7, l. 30 – p. 8, l. 30; Figure 2. The method includes applying (*e.g.*, 204) a first incoming plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, and applying (*e.g.*, 206) a second incoming plaintext block derived from a non-secret entity-identifier independent of the PIN and ciphertext from a cipher block in the CBC chain to a second of the plurality of cipher blocks. *See id.* Lastly, the method includes keying (*e.g.*, 208) the plurality of cipher blocks with a secret PIN Verification Key (PVK) and executing (*e.g.*, 210) the plurality of cipher blocks wherein ciphertext is generated. *See id.*

With regard to independent claim 20, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 20 recites a data security apparatus (*e.g.*, 600) including an enrollment terminal (*e.g.*, 614) configured to accept an entity-selected secret Personal Identification Number (PIN) and to accept (*e.g.*, via 602 and 604) a magnetic stripe card storing a non-secret entity-identifier independent of the PIN. *See* Application, p. 12, ll. 27-30; p. 13, ll.

8-12; Figure 6. The apparatus includes a processor (*e.g.*, 616) coupled to the enrollment terminal that receives the entity-identifier and the PIN, and a memory (*e.g.*, 617) coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to enroll a PIN including linking (*e.g.*, 202) a plurality of cipher blocks in a Cipher Block Chain (CBC), applying (*e.g.*, 204) an incoming first plaintext block derived from the secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, applying (*e.g.*, 206) an incoming second plaintext block derived from the non-secret entity-identifier that is independent of the PIN and ciphertext from a cipher block in the CBC chain, keying (*e.g.*, 208) the plurality of cipher blocks with a secret PIN Verification Key (PVK), and executing (*e.g.*, 210) the cipher blocks resulting in generation of ciphertext PIN Verification Value (PVV) for usage in performing a subsequent PIN verification function. *See id.* at p. 7, l. 30 – p. 8, l. 30; p. 12, l. 27 – p. 13, l. 6; Figures 2 and 6.

With regard to independent claim 28, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 28 recites a data security apparatus including a PIN Verification Value (PVV) database (*e.g.*, 502) configured to store a plurality of PIN Verification Values (PVVs) for enrolled magnetic stripe cards. *See* Application, p. 6, ll. 14-27; p. 7, ll. 10-24; p. 10, ll. 24-34; p. 11, ll. 22-24; p. 12, ll. 8-10 and 20-25; Figures 1A, 1B, 5A, and 5C. The apparatus includes an escrow (*e.g.*, 128, 504) configured to store a plurality of escrow values associated with at least some of the enrolled magnetic stripe cards. *See id.* at p. 7, ll. 10-24; p. 11, ll. 10-11 and 25-27; p. 12, 11. 1- 10; Figures 1B, 5A, and 5B. The apparatus includes a processor (*e.g.*, 616, 712) coupled to the PVV database (*e.g.*, 502) and the escrow (*e.g.*, 504) that receives an entity-identifier, a PIN Verification Value (PVV) associated to the entity-identifier, and at least one escrow value associated to the entity-identifier. *See id.* at p. 12, ll. 30-34; p. 13, ll. 12-15 and 24-26; Figures 6 and 7. Further, the apparatus includes a memory (*e.g.*, 617) coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to recover a PIN including (*e.g.*, 200 but for recovery and not enrollment) linking (*e.g.*,

202) a plurality of cipher blocks in a Cipher Block Chain (CBC), applying (*e.g.*, 204 with PVV instead of PIN) an incoming first plaintext block derived from the PIN Verification Value (PVV) to one of the plurality of cipher blocks, applying (*e.g.*, 206) an incoming second plaintext block derived from the non-secret entity-identifier that is independent of the PIN and ciphertext from a cipher block in the CBC chain, keying (*e.g.*, 208) the plurality of cipher blocks with a secret PIN Verification Key (PVK), and executing the cipher blocks to produce a ciphertext value, and combining the ciphertext value with the at least one escrow value resulting in recovery of the PIN verification function. *See id.* at p. 6, ll. 31-33; p. 7, ll. 10-14; p. 11, ll. 10-11 and 30-32; p. 12, ll. 1-10 and 30-34; Figures 2, 5B, and 6.

With regard to independent claim 29, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 29 recites a data security apparatus including a transaction terminal (*e.g.*, 614, 708) adapted to accept an entity-entered secret Personal Identification Number (PIN') and to accept a magnetic stripe card storing a non-secret entity-identifier independent of the PIN. *See* Application, p. 4, ll. 11-16; p. 6, ll. 4-5; p. 12, ll. 12-17; p.13, ll. 8-13 and 19-25; Figures 5C, 6, and 7. The apparatus also includes a PIN Verification Value (PVV) database (*e.g.*, 502). *See id.* at p. 6, ll. 14-27; p. 7, ll. 10-24; p. 10, ll. 24-34; p. 11, ll. 22-24; p. 12, ll. 8-10 and 20-25; Figures 1A, 1B, 5A, and 5C. Further, the apparatus includes a processor (*e.g.*, 616, 712) communicatively coupled to the transaction terminal that receives the entity-identifier, the PIN', and coupled to the PVV database of for retrieving a PIN Verification Value (PVV) associated with the entity-identifier. *See id.* at p. 12, ll. 30-34; p. 13, ll. 12-15 and 24-26; Figures 6 and 7. The apparatus also includes a memory (*e.g.*, 617) coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to verify the PIN' comprising linking (*e.g.*, 202) a plurality of cipher blocks in a Cipher Block Chain (CBC), applying (*e.g.*, 204 with PIN') an incoming first plaintext block derived from the secret entered Personal Identification Number (PIN') to one of the plurality of cipher blocks, applying (*e.g.*, 206) an incoming second plaintext block derived from the non-secret entity-identifier independent of the PIN' and ciphertext from a cipher block in the CBC chain, keying (*e.g.*, 208) the plurality of cipher blocks with a secret PIN Verification Key (PVK), and executing the cipher blocks resulting in generation of ciphertext transaction PIN Verification Value (PVV'), and comparing the generated PVV' and the retrieved PVV and determining PIN verification based on the comparison. *See id.* at p. 7, l. 30 – p. 8, l. 13; p. 11, ll. 13-16; p. 12, ll. 12-25; p. 12, l. 30 – p. 13, l. 6; Figures 2, 5C, and 6.

With regard to independent claim 30, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 30 recites a transaction system (*e.g.*, 700) including a network (*e.g.*, 702), a plurality of servers (*e.g.*, 704) and/or hosts (*e.g.*, 706) coupled to the network, and a plurality of terminals (*e.g.*, 708) coupled to the servers via the network. *See* Application, p. 13, ll. 17-21; Figure 7. The transaction system includes a plurality of magnetic stripe cards (*e.g.*, 710) enrolled in the transaction system (*e.g.*, 700) and configured for insertion into the on-line terminals (*e.g.*, 708) and performing transactions via the servers (*e.g.*, 704). *See id.* at p. 13, ll. 21-24; Figure 7. The system includes a plurality of processors (*e.g.*, 712) distributed among the servers (*e.g.*, 704), hosts (*e.g.*, 706), and/or the terminals (*e.g.*, 708), at least one of the processors (*e.g.*, 712) being capable of executing PIN verification using a magnetic stripe card (*e.g.*, 710). *See id.* at p. 13, ll. 24-26; Figure 7. The system and processor has a computable readable program code (*e.g.*, 200 logic) embodied therein capable of causing the processor (*e.g.*, 712) to link (*e.g.*, 202) a plurality of cipher blocks in a Cipher Block Chain (CBC), apply (*e.g.*, 204) an incoming first plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, apply (*e.g.*, 206) an incoming second plaintext block derived from a non-secret entity-identifier independent of the PIN and ciphertext from a cipher block in the CBC chain, key (*e.g.*, 208) the plurality of cipher blocks with a secret PIN Verification Key (PVK), and execute (*e.g.*, 210) the cipher blocks resulting in generation of ciphertext. *See id.* at p. 7, l. 30 – p. 8, l. 30; p. 13, ll. 17-26; Figures 2 and 7.

With regard to independent claim 31, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 31 recites a data security apparatus (*e.g.*, 500, 600, 700) including means (*e.g.*, 606, 608, 616, 617, 712) for enrolling a transaction card (*e.g.*, 710) in a data system, and means (*e.g.*, 606, 608, 616, 617, 712) for generating a Personal Identification Number (PIN) Verification Value (PVV) (*e.g.*, stored in 502) for usage (*e.g.*, 200) in Personal Identification Number (PIN) verification. *See* Application, p. 7, l. 30 – p. 8, l. 30; p. 11, ll. 18-25; p. 12, l. 27 – p. 13, l. 26; Figures 2, 5A, 6, and 7. The apparatus includes means (*e.g.*, 606, 608, 616, 617, 712) for linking (*e.g.*, 202) a plurality of cipher blocks in a Cipher Block Chain (CBC), means (*e.g.*, 606, 608, 616, 617, 712) for applying (*e.g.*, 204) an incoming first plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, means (*e.g.*, 606, 608, 616, 617, 712) for applying (*e.g.*, 206) an incoming second plaintext block derived from a non-secret entity-identifier independent of the PIN to another of the plurality of cipher blocks, and means for keying (*e.g.*, 208) the plurality of cipher blocks with a secret PIN Verification Key (PVK). *See id.* at p. 7, l. 30 – p. 8, l. 4; p. 12, l. 27 – p. 13, l. 26; Figures 2, 6, and 7. The apparatus includes means (*e.g.*, 606, 608, 616, 617, 712) for generating a PIN Verification Value (PVV) via operation of a plurality of cipher blocks in the Cipher Block Chain, and means (*e.g.*, 606, 608, 616, 617, 712) for writing the PVV to a transaction card for subsequent PIN verification. *See id.* at p. 12, l. 27 – p. 13, l. 26; Figures 6 and 7.

Dependent Claims 2, 4, 5, 6, 14, 15, 22, and 23

With regard to dependent claim 2, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 2 recites the apparatus (*e.g.*, 100) of claim 1, including a logical operator (*e.g.*, 106A) that exclusive-ORs the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block. *See* Application, p. 4, ll. 14-16; Figure 1A. A first encryptor (*e.g.*, 102A) that encrypts the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block (*e.g.*, 108A). *See id.* at p. 4, ll. 16-20; Figure 1A. A logical operator that exclusive-ORs the second plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block. A second encryptor (*e.g.*, 102B) that encrypts the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block (*e.g.*, 108B). *See id.* at p. 4, ll. 20-23; Figure 1A.

With regard to dependent claim 4, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 4 recites the apparatus of claim 2, including a logical operator (*e.g.*, 122) that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block (*e.g.*, 124). *See* Application, p. 7, ll. 1-8; p. 11, ll. 1-8; Figure 1B.

With regard to dependent claim 5, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 5 recites the apparatus of claim 4, including wherein the PIN verification apparatus (*e.g.*, 120) operates in an irreversible mode that obstructs recovery of the secret PIN. *See* Application, p. 7, ll. 1-12 and 22-24; p. 11, ll. 1-11; Figure 1B.

With regard to dependent claim 6, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 6 recites the apparatus of claim 5, including an escrow storage (*e.g.*, 128, 504, via 126) coupled to the second encryptor (*e.g.*, 102B) that stores the second ciphertext block. *See* Application, p. 7, ll. 12-20; p. 11, ll. 10-11 and 25-28; p. 12, ll. 1-10; Figures 1B, 5A, and 5B.

With regard to dependent claim 14, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 14 recites the method of claim 11, including operating in an irreversible mode (e.g., 120) that obstructs recovery of the secret PIN, exclusive-ORing (e.g., via

106A) the first incoming plaintext block derived from the secret PIN with an initialization vector to produce an initialized block, encrypting (e.g., via 102A) the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block (e.g., via 108A), and exclusive-ORing (e.g., via 106B) the second incoming plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block, encrypting (e.g., via 102B) the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block (e.g., via 108A), exclusive-ORing (e.g., via 122) the first ciphertext block with the second ciphertext block to produce a third ciphertext block (e.g., 124), and supplying the second ciphertext block for PIN verification. *See* Application, p. 4, ll. 14-23; p. 7, ll. 1-8; p. 11, ll. 1-8; Figures 1A and 1B.

With regard to dependent claim 15, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 15 recites the method of claim 14 including storing (e.g., 126) the second ciphertext block in at least one escrow (*e.g.*, 128, 504) to facilitate recovery of the secret PIN. *See* Application, p. 7, ll. 12-20; p. 11, ll. 10-11 and 25-28; p. 12, ll. 1-10; Figures 1B, 5A, and 5B.

With regard to dependent claim 22, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 22 recites the apparatus of claim 20, including wherein the PIN verification function is configured to operate in an irreversible mode (e.g., 120) that obstructs recovery of the secret PIN and the memory (e.g., 617) includes computable readable program code capable of causing the processor to exclusive-OR (e.g., via 106A) the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block, encrypt (e.g., via 102A) the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block (e.g., 108A), exclusive-OR (e.g., via 106B) the second plaintext block derived from the non-secret entity-identifier that is independent of the PIN with the first ciphertext block to produce a chained block, encrypt (e.g., via 102B) the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block (108B), exclusive-OR (e.g., via 122) the first ciphertext block with the second ciphertext block to produce a third ciphertext block (e.g., via 124), and supply the second ciphertext block for PIN verification. *See* Application, p. 4, ll. 14-23; p. 7, ll. 1-8; p. 11, ll. 1-8; Figures 1A, 1B, and 6.

With regard to dependent claim 23, discussions of the recited features can be found at least in the below-cited locations of the specification and drawings. By way of example, claim 23 recites the apparatus of claim 22 including an escrow storage (*e.g.*, 128, 504) communicatively coupled to the transaction system and comprising at least one escrow storage element (*e.g.*, 128, 504), and the memory (e.g., 617) including a computable readable program code capable of causing the processor to store the second ciphertext block in the escrow storage (*e.g.*, 128, 504) in at least one secret escrow share to facilitate recovery of the secret PIN. *See* Application, p. 7, ll. 12-20; p. 11, ll. 10-11 and 25-28; p. 12, ll. 1-10; Figures 1B, 5A, 5B, and 6.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. First Ground of Rejection for Review on Appeal

The Appellants respectfully urge the Board to review and reverse the Examiner's first ground of rejection in which the Examiner rejected claims 1-3, 7-10, 11-13, 16-21 and 24-31 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 4,924,514 by Matyas (hereinafter "Matyas") and in view of an IBM Research Report by Coppersmith (hereinafter "Coppersmith").

B. Second Ground of Rejection for Review on Appeal

The Appellants respectfully urge the Board to review and reverse the Examiner's second ground of rejection in which the Examiner rejected claims 4-5 under 35 U.S.C. §

103(a) as being unpatentable over Matyas in view of Coppersmith and further in view of U.S. Patent No. 1,310,719 by Vernam (hereinafter "Vernam").

C. Third Ground of Rejection for Review on Appeal

The Appellants respectfully urge the Board to review and reverse the Examiner's third ground of rejection in which the Examiner rejected claims 14 and 22 under 35 U.S.C. § 103(a) as being unpatentable over Matyas in view of Coppersmith as applied to claims 11 And 20 above, and further in view of Vernam.

D. Fourth Ground of Rejection for Review on Appeal

The Appellants respectfully urge the Board to review and reverse the Examiner's fourth ground of rejection in which the Examiner rejected claims 6, 15, and 23 under 35 U.S.C. § 103(a) as being unpatentable over Matyas in view of Coppersmith in view of Vernam, and further in view of U.S. Patent No. 4,747,050 to Brachti et al. (hereinafter "Brachti").

7. ARGUMENT

As discussed in detail below, the Examiner has improperly rejected the pending claims. Further, the Examiner has misapplied long-standing and binding legal precedents and principles in rejecting the claims under 35 U.S.C. § 103(a). Accordingly, the Appellants respectfully request full and favorable consideration by the Board, as the Appellants assert that claims 1-31 are currently in condition for allowance.

A. Ground of Rejection No. 1

The Appellants respectfully traverse the rejection of claims 1-3, 7-10, 11-13, 16-21 and 24-31 under 35 U.S.C. § 103(a) as being unpatentable over Matyas in view of Coppersmith. Claims 1, 11, 20, and 28-31 are independent.

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka,* 180 U.S.P.Q. 580 (C.C.P.A. 1974). Although a showing of obviousness under 35 U.S.C. § 103 does not require an express teaching, suggestion or motivation to combine prior art references, such a showing has been described by the Federal Circuit as providing a "helpful insight" into the obviousness inquiry. *KSR Int'l. Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 U.S.P.Q.2d 1385 (2007). Moreover, obviousness cannot be established by a mere showing that each claimed element is present in the prior art. *Id.* The Examiner must cite a compelling reason why a person having ordinary skill in the art would combine known elements in order to support a proper rejection under 35 U.S.C. § 103. *Id.*

Deficiencies of the Rejection of Independent Claims 1, 11, 20, and 28-31

Independent claims 1, 11, 20, and 28-31 generally recite input text blocks including a first input text block that receives a first plaintext block derived from a secret PIN and a second input text block that receives a second plaintext block derived from a non-secret entity-identifier that is *independent* of the PIN. In the present specification, the entity-identifier's characteristic independence from the PIN is generally discussed and further stressed in explaining that the institution that enrolls the customer account (the entity-identifier) does not possess the PIN. *See, e.g.*, Application, p. 11. l. 30 – p. 12, l. 10; Figures 1A and 1B.

In contrast, Matyas describes a technique where a first input to the cryptographic algorithm is the PIN, but a second input is an IBM 3624-formatted PIN that is derived from validation data and a PIN validation key (which is derived from the PIN and which is specifically contrary to the present claims). *See* Matyas, col. 22, ll. 50-54. Thus, the technique disclosed by Matyas results in the difficulties raised by paragraph [0007] in the background section of the present specification:

> If a PIN is compromised, then an adversary can use the PIN offset to compute a new PIN chosen by the customer. Accordingly, selection of the new PIN does not attain security once a PIN is compromised. The only way to recover security is for the bank or other issuing entity to change either the customer account number or the bank's PIN verification key. Changing the customer account number is difficult for the bank, and changing the PIN verification key is even more difficult. Accordingly, an easy attack against that PIN is available.

Application, p. 2, ll. 14-21.

In the Response to Arguments section of the Final Office Action, the Examiner stated incorrectly that the Matyas "second input is an intermediate PIN <u>which is independent</u> from the customer selected PIN." *See* Final Office Action, p. 2 (emphasis in original). The Examiner quoted from paragraph [0005] in the background section of the present specification, stating "[o]ne technique determines a PIN offset as a . . . difference of a natural PIN and a customer selected PIN." Final Office Action (citing Application, para. [0005], p. 2, ll. 14-21). The Examiner concluded that:

> As the Natural PIN (the Intermediate PIN in Matyas) is the PAN encrypted with the PGK. As the natural PIN is distinct from the customer selected PIN, the cited second input is already <u>independent of the PIN</u>. Therefore the argument that Matyas does not teach wherein the second input block is independent of the (secret) PIN is found to be unpersuasive.

Final Office Action, p. 2 (emphasis in original).

However, the Matyas technique utilizes a PIN validation key, which is derived from the PIN. Moreover, the characterization of the Matyas intermediate PIN as a natural PIN supports the Appellants' argument that the Matyas intermediate PIN is not independent of the secret PIN. Indeed, the security problems associated with employment of a natural PIN is directly addressed by the present specification (see background) and specifically avoided in the claims. *See* Application, p. 2, ll. 1-7 and 14-

21. As appreciated by one of ordinary skill in the art, the Matyas IBM 3624 approach (with or without an offset) provides for the issuing bank to generate the customer or secret PIN.

As for the secondary reference, Coppersmith is directed to "a new mode of multiple encryption." *See* Coppersmith, Abstract (p. 1). Coppersmith does not disclose one of the cryptographic algorithm's inputs being an identity-identifier, which is independent of the PIN, as claimed, nor did the Examiner allege so.

For at least the reasons discussed above, the cited references, alone or in any hypothetical combination, fail to disclose all of the elements recited in independent claims 1, 11, 20, and 28-31. Accordingly, these claims are allowable over the cited combination. For at least the same reasons, the dependent claims 2-10, 12-19, and 21-27 are allowable over the cited references. Accordingly, the Appellants respectfully request that the Board reverse the rejection of claims 1-3, 7-10, 11-13, 16-21 and 24-31under 35 U.S.C. § 103(a).

B. Ground of Rejection No. 2

The Appellants respectfully traverse the rejection of dependent claims 4-5 under 35 U.S.C. § 103(a) as being unpatentable over Matyas in view of Coppersmith and further in view of Vernam.

Initially, it should be noted that Vernam, which is directed to secrecy in the transmission of telegraph messages, does not remedy the deficiencies of Matyas and Coopersmith discussed above with respect to independent claim 1. *See* Vernam, col. 1, ll. 8-17. Claims 4 and 5 are patentable by virtue of their dependency on an allowable base claim. Further, claims 4 and 5 are also patentable over the cited combination because of the subject matter they separately recite.

Deficiencies of the Rejection of Claims 4 and 5

Claim 4 recites "a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block." The Examiner acknowledged that Matyas and Coppersmith do not teach a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block, but stated that Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext. However, Vernam does not teach first and second ciphertexts that are formed and combined to produce a ciphertext, but rather merely discloses a combination of a plaintext block with a ciphertext block. Accordingly, the combination of Matyas, Coppersmith and Vernam, does not combine signals and thus does not operate as claimed by the Appellants.

In the Response to Arguments section of the Final Office Action, the Examiner stated with regard to claim 4 that "Vernam teaches taking two inputs and using XOR to produce a cipher text," and that "[w]hether or not the inputs are cipher text or plaintext should be directed to the Coppersmith reference." Final Office Action, p. 3. However, the references, whether taken alone or in combination, do not disclose "a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block," as claimed. The Examiner has not met the burden of establishing a *prima facie* case of obviousness. For this additional reason, claim 4 and its dependent claim 5 is patentable over the cited combination.

Additional Deficiencies of the Rejection of Claim 5

Claim 5 recites "wherein the PIN verification apparatus operates in an irreversible mode that obstructs recovery of the secret PIN." Conversely, the combination of Matyas, Coppersmith, and Vernam neither describes nor hints of obstructing the recovery of the secret PIN from the second ciphertext block as claimed or operation in the irreversible mode as claimed. Further, the Appellants traverse the Examiner's contention that "[i]t is *inherent* that a PIN verification apparatus operates in an irreversible mode when the secret key is not possessed." *See* Final Office Action, p. 8 (emphasis added). To be sure, the references do not teach an irreversible mode, as claimed. Further, techniques taught by the references facilitate regeneration of the secret PIN, contrary to claim 5. For example, as appreciated by one of ordinary skill in the art, the Matyas IBM 3624 approach (with or without an offset) provides for the issuing bank to generate the customer or secret PIN. For this additional reason, claim 4 and its dependent claim 5 is patentable over the cited combination. For this additional reason, claim 5 is patentable over the cited combination.

In view of the foregoing, dependent claims 4 and 5 are patentable over the cited combination. In view of the foregoing, the cited references, alone or in any hypothetical combination, fail to disclose all of the elements recited in dependent claims 4 and 5. Therefore, these claims 4 and 5 are allowable over the cited references. Accordingly, the Appellants respectfully request that the Board reverse the rejection of claims 4 and 5 under 35 U.S.C. § 103(a).

D. Ground of Rejection No. 3

The Appellants respectfully traverse the rejection of dependent claims 14 and 22 under 35 U.S.C. § 103(a) as being unpatentable over Matyas in view of Coppersmith as applied to claims 11 and 20 above, and further in view of Vernam.

As indicated, Vernam does not remedy the deficiencies of Matyas and Coppersmith, as discussed above with respect to the independent claims. Therefore, claims 14 and 22 are patentable over the instant combination because of their dependency on an allowable base claim. In addition, claims 14 and 22 are also patentable because of the subject matter they separately recite.

Deficiencies of the Rejection of Claims 14 and 22

For example, claim 14 recites, *inter alia*, “operating in an irreversible mode that obstructs recovery of the secret PIN.” Conversely, as previously noted, the cited references are devoid of this feature. Indeed, techniques taught by the references facilitate regeneration of the secret PIN, contrary to claim 5. For example, as appreciated by one of ordinary skill in the art, the Matyas IBM 3624 approach (with or without an offset) provides for the issuing bank to generate the customer or secret PIN. Further, claims 14 and 22 recite, *inter alia*, supplying "the second ciphertext block for PIN verification." The references do not disclose supplying a second ciphertext block for PIN verification, as claimed. For these additional reasons claims 14 and 22 are patentable over the cited combination.

In view of the foregoing, the cited references, alone or in any hypothetical combination, fail to disclose all of the elements recited in dependent claims 14 and 22. Therefore, these claims are allowable over the cited combination. Accordingly, the Appellants respectfully request that the Board reverse the rejection of claims 14 and 22 under 35 U.S.C. § 103(a).

E. Ground of Rejection No. 4

The Appellants respectfully traverse the rejection of dependent claims 6, 15, and 23 under 35 U.S.C. § 103(a) as being unpatentable over Matyas in view of Coppersmith and Vernam, and further in view of Brachti.

Brachti does not remedy the deficiencies of Matyas, Coppersmith, and Vernam as discussed above with respect to the independent claims (or with respect to dependent claims 5, 14, and 22). Therefore, claims 6, 15, and 23 are patentable over the instant combination because of their dependency on allowable base claims. In addition, at least claims 15 and 23 are also patentable because of the subject matter they separately recite.

Deficiencies of the Rejection of Claims 15 and 23

Claim 15 recites "storing the second ciphertext block in at least one escrow to facilitate recovery of the secret PIN." Claim 23 recites "an escrow storage communicatively coupled to the transaction system and comprising at least one escrow storage element; and the memory further comprises a computable readable program code capable of causing the processor to store the second ciphertext block in the escrow storage in at least one secret escrow share to facilitate recovery of the secret PIN."

In contrast, while Brachti discloses the general concept of escrow storage, the combined references do not teach storing a ciphertext block in the escrow storage to *facilitate recovery of the secret PIN.* Further, the Examiner acknowledged that Matyas, Coppersmith, and Vernam do not disclose these features. Final Office Action, p. 22.

In view of the foregoing, the cited references, alone or in any hypothetical combination, fail to disclose all of the elements recited in dependent claims 6, 15, and 23. Therefore, these claims are allowable over the cited combination. Accordingly, the Appellants respectfully request that the Board reverse the rejection of claims 6, 15, and 23under 35 U.S.C. § 103(a).

G. Request for Reversal of the Rejections

In view of the reasons set forth above, the Appellants respectfully request the Board to reverse the rejections of claims 1-31 under 35 U.S.C. § and 103(a).

Conclusion

The Appellants respectfully submit that all pending claims are in condition for allowance. However, if the Examiner or Board wishes to resolve any other issues by way of a telephone conference, the Examiner or Board is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: May 24, 2010

/Nathan E. Stacy/
Nathan E. Stacy
Reg. No. 52,249
International IP Law Group, P.C.
(832) 375-0200

CORRESPONDENCE ADDRESS:

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
Fort Collins, Colorado 80528

8. APPENDIX OF CLAIMS ON APPEAL

1. A Personal Identification Number (PIN) verification apparatus comprising:
a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a secret PIN Verification Key (PVK);
a first input block coupled to a first cipher block in the CBC chain that receives a first plaintext block derived from a secret Personal Identification Number (PIN); and
a second input block coupled to a second cipher block in the CBC chain that receives a second plaintext block derived from a non-secret entity-identifier independent of the PIN and receives ciphertext from a cipher block in the CBC chain.

2. The apparatus according to Claim 1 further comprising:
a logical operator that exclusive-ORs the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;
a first encryptor that encrypts the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;
a logical operator that exclusive-ORs the second plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block; and
a second encryptor that encrypts the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block.

3. The apparatus according to Claim 2 wherein:
the PIN verification apparatus operates in a reversible mode that recovers the secret PIN from the second ciphertext block.

4. The apparatus according to Claim 2 further comprising:

a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block.

5. The apparatus according to Claim 4 wherein:

the PIN verification apparatus operates in an irreversible mode that obstructs recovery of the secret PIN.

6. The apparatus according to Claim 5 further comprising:

an escrow storage coupled to the second encryptor that stores the second ciphertext block.

7. The apparatus according to Claim 1 further comprising:

the plurality of cipher blocks that encrypt data according to a triple Data Encryption Standard (3-DES).

8. The apparatus according to Claim 1 further comprising:

a format converter coupled to a cipher block in the CBC chain that converts hexadecimal digit ciphertext to a decimal result by receiving in sequence the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV).

9. The apparatus according to Claim 1 further comprising:

the plurality of cipher blocks that encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

10. The apparatus according to Claim 1 further comprising:

a first formatter that constructs a first incoming plaintext block from a concatenation of a length digit, x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and

a second formatter that constructs a second incoming plaintext block independent of the PIN from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16- y times.

11. A method for Personal Identification Number (PIN) verification comprising:

linking a plurality of cipher blocks in a Cipher Block Chain (CBC);

applying a first incoming plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks;

applying a second incoming plaintext block derived from a non-secret entity-identifier independent of the PIN and ciphertext from a cipher block in the CBC chain to a second of the plurality of cipher blocks;

keying the plurality of cipher blocks with a secret PIN Verification Key (PVK); and

executing the plurality of cipher blocks wherein ciphertext is generated.

12. The method according to Claim 11 further comprising:

encrypting data according to a triple Data Encryption Standard (3-DES) using a plurality of cipher blocks.

13. The method according to Claim 11 wherein the PIN verification method is capable of further comprises:

operating in a reversible mode that enables recovery of the secret PIN;

exclusive-ORing the first incoming plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

exclusive-ORing the second incoming plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block;

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; and

supplying the second ciphertext block for PIN verification.

14. The method according to Claim 11 wherein the PIN verification method further comprises:

operating in an irreversible mode that obstructs recovery of the secret PIN;

exclusive-ORing the first incoming plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

exclusive-ORing the second incoming plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block;

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block;

exclusive-ORing the first ciphertext block with the second ciphertext block to produce a third ciphertext block; and

supplying the second ciphertext block for PIN verification.

15. The method according to Claim 14 further comprising:

storing the second ciphertext block in at least one escrow to facilitate recovery of the secret PIN.

16. The method according to Claim 11 further comprising:
converting hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) to a decimal result by receiving in sequence the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV); and
using the PVV for PIN verification.

17. The method according to Claim 11 further comprising:
supplying hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV).

18. The method according to Claim 11 further comprising:
a plurality of cipher blocks that encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

19. The method according to Claim 11 further comprising:
constructing the first the first incoming plaintext block from a concatenation of a length digit, x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and
constructing a second the second incoming plaintext block from a
concatenation of y hexadecimal digits of the non-secret entity-identifier
with a pad character that is repeated 16-y times wherein the second incoming plaintext block is independent of the PIN.

20. A data security apparatus comprising:

an enrollment terminal configured to accept an entity-selected secret Personal Identification Number (PIN) and a magnetic stripe card storing a non-secret entity-identifier independent of the PIN;

a processor coupled to the enrollment terminal that receives the entity-identifier and the PIN; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to enroll a PIN comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming first plaintext block derived from the secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, applying an incoming second plaintext block derived from the non-secret entity-identifier that is independent of the PIN and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK), and

executing the cipher blocks resulting in generation of ciphertext PIN Verification Value (PVV) for usage in performing a subsequent PIN verification function.

21. The apparatus according to Claim 20 wherein the PIN verification function is configured to operate in a reversible mode that enables recovery of the secret PIN and the memory further comprises:

a computable readable program code capable of causing the processor to exclusive-OR the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a computable readable program code capable of causing the controller to encrypt the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the second plaintext block derived from the non-secret entity-identifier that is independent of the PIN with the first ciphertext block to produce a chained block;

a computable readable program code capable of causing the controller to encrypt the chained block using triple Data Encryption Standard (3- DES) encryption to produce a second ciphertext block; and

a computable readable program code capable of causing the controller to supply the second ciphertext block for PIN verification.

22. The apparatus according to Claim 20 wherein the PIN verification function is configured to operate in an irreversible mode that obstructs recovery of the secret PIN and the memory further comprises:

a computable readable program code capable of causing the processor to exclusive-OR the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a computable readable program code capable of causing the controller to encrypt the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the second plaintext block derived from the non-secret entity-identifier that is independent of the PIN with the first ciphertext block to produce a chained block;

a computable readable program code capable of causing the controller to encrypt the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the first ciphertext block with the second ciphertext block to produce a third ciphertext block; and

a computable readable program code capable of causing the controller to supply the second ciphertext block for PIN verification.

23. The apparatus according to Claim 22 further comprising:

an escrow storage communicatively coupled to the transaction system and comprising at least one escrow storage element; and

the memory further comprises a computable readable program code capable of causing the processor to store the second ciphertext block in the escrow storage in at least one secret escrow share to facilitate recovery of the secret PIN.

24. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to convert hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) to a decimal result by receiving in sequence the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV); and

a computable readable program code capable of causing the processor to write the PVV to a magnetic stripe card or a smart card.

25. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to store hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV) in a storage element.

26. The apparatus according to Claim 20 wherein:

the plurality of cipher blocks encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

27. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to construct the first incoming plaintext block from a concatenation of a length digit and x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and

a computable readable program code capable of causing the processor to construct the second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times wherein the second incoming plaintext block is independent of the PIN.

28. A data security apparatus comprising:

a PIN Verification Value (PVV) database configured to store a plurality of PIN Verification Values (PVVs) for enrolled magnetic stripe cards;

an escrow configured to store a plurality of escrow values associated with at least some of the enrolled magnetic stripe cards; and

a processor coupled to the PVV database and the escrow that receives an entity-identifier, a PIN Verification Value (PVV) associated to the entity-identifier, and at least one escrow value associated to the entity-identifier; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to recover a PIN comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming first plaintext block derived from the PIN Verification Value (PVV) to one of the plurality of cipher blocks, applying an incoming second plaintext block derived from the non-secret entity-identifier that is independent of the PIN and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK), executing the cipher blocks to produce a ciphertext value, and combining the ciphertext value with the at least one escrow value resulting in recovery of the PIN verification function.

29. A data security apparatus comprising:

a transaction terminal adapted to accept an entity-entered secret Personal Identification Number (PIN') and a magnetic stripe card storing a non-secret entity-identifier independent of the PIN;

a PIN Verification Value (PVV) database;

a processor communicatively coupled to the transaction terminal that receives the entity-identifier, the PIN', and coupled to the PVV database of for retrieving a PIN Verification Value (PVV) associated with the entity-identifier; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to verify the PIN' comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming first plaintext block derived from the secret entered Personal Identification Number (PIN') to one of the plurality of cipher blocks, applying an incoming second plaintext block derived from the non-secret entity-identifier independent of the PIN' and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK),

executing the cipher blocks resulting in generation of ciphertext transaction PIN Verification Value (PVV'); comparing the generated PVV' and the retrieved PVV; and determining PIN verification based on the comparison.

30. A transaction system comprising:

a network;

a plurality of servers and/or hosts coupled to the network;

a plurality of terminals coupled to the servers via the network;

a plurality of magnetic stripe cards enrolled in the transaction system and configured for insertion into the on-line terminals and performing transactions via the servers; and

a plurality of processors distributed among the servers, hosts, and/or the terminals, at least one of the processors being capable of executing PIN verification using a magnetic stripe card and having a computable readable program code embodied therein capable of causing the processor to link a plurality of cipher blocks in a Cipher Block Chain (CBC), apply an incoming first plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, apply an incoming second plaintext block derived from a non-secret entity-identifier independent of the PIN and ciphertext from a cipher block in the CBC chain, key the plurality of cipher blocks with a secret PIN Verification Key (PVK), and execute the cipher blocks resulting in generation of ciphertext.

31. A data security apparatus comprising:

means for enrolling a transaction card in a data system; and

means for generating a Personal Identification Number (PIN) Verification Value (PVV) for usage in Personal Identification Number (PIN) verification further comprising:

means for linking a plurality of cipher blocks in a Cipher Block Chain (CBC);

means for applying an incoming first plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks;

means for applying an incoming second plaintext block derived from a non-secret entity-identifier independent of the PIN to another of the plurality of cipher blocks;

means for keying the plurality of cipher blocks with a secret PIN Verification Key (PVK); and means for generating a PIN Verification Value (PVV) via operation of a plurality of cipher blocks in the Cipher Block Chain; and

means for writing the PVV to a transaction card for subsequent PIN verification.

9. **EVIDENCE APPENDIX**

None.

10. **RELATED PROCEEDINGS APPENDIX**

None.